Amendments to the Claim of Priority:

On Page 1, line 1, please replace the paragraph following the header CROSS-REFERENCES TO RELATED APPLICATIONS with the following:

This application is a continuation of U.S. Patent Application No. 09/497,393 filed February 3, 2000, now U.S. Patent No. _____, which claims the benefit of priority on U.S. Provisional Patent Application No. 60/126,805 filed March 30, 1999.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Please cancel claims 1-33. Following is a complete set of claims as amended with this Response.

1-33. (Cancelled).

34. (New) A method comprising:

receiving digital program data in a scrambled format by a descrambler integrated circuit;

receiving control data in an encrypted format by the descrambler integrated circuit;

decrypting the encrypted control data entirely within the descrambler integrated circuit using a key permanently stored in the descrambler integrated circuit; and

descrambling the scrambled digital program data in the descrambler integrated circuit using the decrypted control data.

35. (New) The method of claim 34, wherein the control data includes a service key to descramble the scrambled digital program data if the digital program data belongs to a selected group of programs each of which is capable of being descrambled by the service key.

36. (New) The method of claim 34, wherein prior to receiving the scrambled digital program data, the method further comprising programming the permanent key into a memory at manufacture of a digital device including the descrambler integrated circuit, the key being non-modifiable.

37. (New) The method of claim 34, wherein prior to receiving the encrypted control data, the method further comprising sending a request for the encrypted control data to a headend.

38. (New) The method of claim 37, wherein the request is sent over an out-of-band channel.

39. (New) The method of claim 37, wherein the request is transmitted in accordance with a Data Over Cable Service Interface Specification (DOCSIS) cable transmission protocol.

40. (New) The method of claim 39, wherein the out-of-band request includes (i) an address of a digital device implemented with the descrambler integrated circuit and (ii) an identifier of a channel at which the digital program data is received.

41. (New) The method of claim 34, wherein prior to receiving the encrypted control data, the method further comprising encrypting the control data in a smart card using a key stored in a register circuit of the smart card, the key stored in the register circuit of the smart card being equivalent to the key permanently stored in the descrambler integrated circuit.

42. (New) The method of claim 41, wherein prior to receiving the encrypted control data, the method further comprising receiving the encrypted control data by an interface removably coupled to the smart card, the interface being part of a digital receiver implemented with the descrambler integrated circuit.

43. (New) The method of claim 42, wherein the interface includes an expansion slot built into the digital receiver.

44. (New) The method of claim 34, wherein the digital program data comprises audio and visual data.

45. (New) The method of claim 44, wherein the digital program data further comprises system information including one or more of a program name, broadcast time, and source of the digital program data.

46. (New) The method of claim 34, wherein the digital program data comprises an entitlement management message to deliver privileges to a digital receiver implemented with the descrambler integrated circuit.

47. (New) The method of claim 34, wherein the digital program data comprises an entitlement control message including at least one of an identifier of a channel being tuned for receipt of the scrambled digital program data, an identifier to locate the key stored in the descrambler integrated circuit, and an identifier of the digital program data being broadcast.

48. (New) A descrambler integrated circuit adapted for implementation in a conditional access unit, comprising:

a memory to permanently store a key uniquely assigned to the descrambler integrated circuit, the memory being a one-time programmable non-volatile memory;

decryption logic coupled to the memory, the decrypt logic to decrypt the encrypted data using the key completely within the descrambler integrated circuit without accessing any information external to the decryption logic; and

a descrambler coupled to the decryption logic, the descrambler to descramble incoming scrambled, digital program data within the descrambler integrated circuit using data recovered by decrypting the encrypted data.

49. (New) The descrambler integrated circuit of claim 48, wherein the memory is a one-time programmable register.

50. (New) The descrambler integrated circuit of claim 48, wherein the encrypted data is a service key in an encrypted format being valid for a prescribed period of time, the encrypted service key, when decrypted, to descramble the scrambled digital program data if the digital program data belongs to a selected group of programs each of which capable of being descrambled by the service key.

51. (New) The descrambler integrated circuit of claim 50 being controlled by a processor in communications with a transmitter implemented within the conditional access unit, the transmitter to transmit a request for the service key in the encrypted format to a headend.

52. (New) The descrambler integrated circuit of claim 51, wherein the request for the service key is transmitted over an out-of-band channel.

53. (New) The descrambler integrated circuit of claim 48, wherein the key is stored within the memory during manufacturer, at which time, the key and a serial number associated with the conditional access unit implemented with the descrambler integrated circuit are recorded by storage external from the descrambler integrated circuit.

54. (New) A method comprising:

receiving digital program data in a scrambled format by a descrambler integrated circuit;

decrypting control data stored in an encrypted format entirely within the descrambler integrated circuit using a one-time programmable key permanently stored in the descrambler integrated circuit; and

descrambling the scrambled digital program data in the descrambler integrated circuit using the decrypted control data.

55. (New) The method of claim 54, wherein prior to receiving the scrambled digital program data, the method further comprising:

requesting the control data from a headend, the control data being a service key that, after being decrypted, to descramble the descrambled digital program data on a channel tuned to by a digital device implemented with the descrambler integrated circuit.

56. (New) An apparatus comprising:

a first interface to receive encrypted data; and

a descrambler integrated circuit in communication with the first interface, the descrambler integrated circuit comprises

a memory to permanently store a key uniquely assigned to the descrambler integrated circuit, the memory being a one-time programmable non-volatile memory,

decryption logic to decrypt the encrypted data using the key completely within the descrambler integrated circuit without accessing any information external to the decryption logic, and

a descrambler to descramble incoming scrambled, digital content within the descrambler integrated circuit using data recovered by decrypting the encrypted data.

57. (New) The apparatus of claim 56, wherein the first interface includes an expansion slot to receive a smart card.

58. (New) The apparatus of claim 56, wherein the memory of the descrambler integrated circuit is a register that can be only programmed once.

59. (New) The apparatus of claim 56 further comprising a processor coupled to the first interface.

60. (New) The apparatus of claim 59, further comprising an internal memory device coupled to the processor, the internal memory to store an encrypted service key being the encrypted data, the service key, when decrypted, to descramble the scrambled, digital program data if the digital program data belongs to a selected group of programs each of which capable of being descrambled by the service key.

61. (New) The apparatus of claim 56, wherein the encrypted data is an encrypted control word.

62. (New) The apparatus of claim 56, wherein the encrypted data is a service key in an encrypted format being valid for a prescribed period of time, the service key, when decrypted, to descramble the scrambled, digital program data if the digital program data belongs to a selected group of programs each of which capable of being descrambled by the service key

63. (New) The apparatus of claim 62 further comprising a transmitter to transmit a request for the service key in the encrypted format over an out-of-band channel directed to a headend.

64. (New) The apparatus of claim 56, wherein the memory of the descrambler integrated circuit is configured to prevent the permanent key from being overwritten or from being read by a source external to the descrambler integrated circuit.

65. (New) The apparatus of claim 56, wherein the key and a serial number of the apparatus are recorded and stored externally from the descrambler integrated circuit.

66. (New) The apparatus of claim 56, wherein the descrambler integrated circuit is devoid of a central processing unit, software or firmware.

67. (New) The apparatus of claim 56 is a conditional access unit.